TERME DE RÉFÉRENCE

POUR LE RECRUTEMENT D'UN CABINET POUR ASSURER L'AUDIT DES SYSTÈMES D'INFORMATION DU TRÉSOR PUBLIC DE MADAGASCAR

1. Contexte

Le Trésor public exerce une multitude de missions, revêtant un caractère hautement stratégique, au sein du Ministère de l'Economie et des Finances (MEF). Ces missions sont définies par l'article 38 du décret n°2019-093 fixant les attributions et l'organisation du MEF. Elles se répartissent globalement en trois types :

- Des missions économiques, conférant au Trésor public un rôle central dans la coordination des politiques macroéconomiques nationales ; dans les secteurs réels finances publiques monétaires extérieurs et d'en préparer les documents de négociation de financement avec les organismes internationaux.
- Des missions financières, consistant à : participer à l'élaboration et à la conduite de la politique financière nationale, régionale et internationale de l'Etat ; assurer la gestion de la dette (intérieure et extérieure), ainsi que les dons et les aides extérieurs ; gérer la trésorerie de l'Etat ; définir et mettre en œuvre la politique d'inclusion financière ; gérer le portefeuille de l'Etat ; assurer la mise en place et le fonctionnement d'un marché financier à Madagascar ; assurer le contrôle et le développement du secteur des assurances.
- Des missions comptables, consistant à : élaborer et mettre en place la réglementation en matière de comptabilité publique ; assurer la gestion financière et comptable de l'Etat, des collectivités et des établissements publics.

De par ses missions, le Trésor public se trouve au carrefour de l'ensemble des flux financiers et comptables de l'Etat, et de ses démembrements. Pour gérer ces flux et traiter le volume des données qu'ils génèrent, il s'appuie sur une multitude de systèmes d'informations cloisonnés, handicapant l'efficacité de son organisation. Ces systèmes d'information constituent le support principal de paiement des dépenses, de perception des recettes dans la sphère comptable et renforce le contrôle et le suivi des opérations sous tutelle pour les missions financières et économiques.

Ces systèmes d'informations bien que redondants et multiples ne couvrent pas la totalité des processus métiers. Parfois, des étapes d'interventions manuelles sont nécessaire afin d'obtenir les résultats escomptés.

Pour chaque mission du Trésor, il est recensé des « Systèmes Intégrés de Gestion » (SIG) dont les intervenants sont variés (Trésor, Douanes, Banques, Opérateur économique, Impôts, Ordonnateurs et Comptables, GAC, etc.) complétés par des applications de gestion en interne conçus selon les attributions/besoins de chaque département.

La modernisation de la gestion de la trésorerie de l'Etat requiert des solutions de portée mondiale suivant les normes et standards en vigueur. A cet effet, il est impératif de connaître exactement les forces et les faiblesses des systèmes existants afin de pouvoir tendre vers un système fiable et répondant parfaitement au contexte malgache ainsi qu'aux besoins des utilisateurs et des autorités.

Dans cette optique, le Trésor public requiert les services d'un expert international pour la réalisation d'un audit des systèmes d'informations actuels.

2. Enjeux et objectifs de la mission

La mission a pour but d'analyser le fonctionnement des SI actuels pour en identifier les forces et les faiblesses en termes de performance des applications et de la sécurité des données et des systèmes techniques et matériels.

Cette mission permettra au Trésor public de connaître exactement les directives à suivre en termes d'organisation, d'infrastructure et de sécurité informatique.

3. Objet de la prestation

3;1. Périmètre

Le consultant fera un audit sur les systèmes informatiques utilisés actuellement par les divers départements du Trésor public, répertoriés comme suit:

Département	SIG		Autres applications / logiciels/ site web	
	Nom	Objet	Nom	Objet
DOF	SIGOC Sous technologie	Logiciel de gestion des opérations de change à Madagascar	OPBE	Gestion des amendes
				Gestion de portefeuille
				Base de données de l'inclusion financière
			mada.inclusionfin.mg	Site web du secteur de l'inclusion financière
DE			SEB	Suivi des exécutions budgétaires
			SE2	Suivi des dossiers juridiques et contentieux
			Courriers	Gestion des courriers
			Stock	Gestion des fourniture et consommables
			RH	Gestion du personnel : congé et fiche de poste
			Consolidation	OGT
DDP	SYGADE 6	Système de gestion et d'analyse de la dette mise au point par CNUCED		
			SIGFP Recette	
			Système de Gestion de BTF-Fihary	Système de gestion des titres publiques BTF Fihary
			Gestion Ordre de recette	Application permettant d'Enregistrer/Editer les tirages des fonds (dettes extérieures)
DBIFA			SIGDBIFA	Gestion des courriers, personnel, affaires et détournement des deniers publics

Département	SIG		Autres applications / logiciels/ site web	
	Nom	**Objet**	**Nom**	**Objet**
	SIG			
	Nom	**Objet**		
DCP	SPECL	Logiciel développé en externe destiné au traitement informatisé des opérations relatives aux crédits carburants dans le cadre du SPECL.		
	SALOHY	Plateforme regroupant plusieurs applications développées en interne Ø Ticket de mandatement Ø Guichet unique Ø Gestion des nomenclatures des pièces Ø Gestion des comptes tiers Ø Pré-engagement Ø Reporting Ø ACPDC Ø Appel de fonds Ø Jasper Ø Centralisation Ø Bibliothèque numérique		
	SIIGFP	Ø LCAD, Ø TRANSFERT Ø CAISSE Ø COMPTA		
	INFO	Gestion des identités des utilisateurs inscrits, responsabilités/roles, édition des décisions, suivi des dossiers de mandatement, consultation des situations relative aux crédits SPECL		
	PORTAIL	Interfaçage et complément opérationnel du SPECL pour les compagnies pétrolières, gérants, suivi des situations et transactions, paiement factures SPECL, remboursement TVA/APP		
	RECETTE NON FISCALE	Traitement des recettes non fiscales avant émission des titres		
	CTD	Application pour le traitement des opérations relatives à la dotation des subventions des Régions et des Communes.		
	EPN	Application dédiée au traitement informatisé des opérations budgétaires et comptables des EPN : saisie du budget, suivi de l'exécution budgétaire, décaissement et encaissement, comptabilité		
DGT/SAF	-	Logiciel de base de données du personnel et traitement associé En cours : Suivi des traitements de dossiers		

Département	SIG		Autres applications / logiciels/ site web	
	Nom	Objet	Nom	Objet
DGT/SCRP		Gestion su Site web et intranet du Trésor Public		

Pour les sites d'informations et de communication, le Trésor public dispose de :

- Un site internet pour le grand public
- Un site intranet pour le personnel uniquement
- Un système de messagerie

L'audit sera axé sur les domaines ci-dessous et sur les domaines qu'il jugera pertinents et importants, pour la réalisation de l'atteinte de l'objectif de sa prestation :

a.L'architecture applicative

Évaluer l'efficacité de l'architecture applicative pour la cohésion des modules, la bonne gouvernance des données, l'interaction avec des systèmes tiers.

b.L'architecture technique

Évaluer la solution technique et son adéquation par rapport aux exigences communes de l'état de l'art en termes de performances, sécurité etc.

c.L'architecture physique

Évaluer l'architecture physique et sa capacité à répondre au niveau de services et aux exigences de sécurité requis.

d. L'architecture opérationnelle

Évaluer l'architecture opérationnelle et sa capacité à répondre aux exigences en termes de supervision, métrologie (recueil et suivi de données de performance), sauvegarde et gestion des environnements (processus et interactions pour le passage entre les différents environnements de la qualification à la production).

3;2. Exigences

- **Norme**

  Organiser la démarche en se référant aux normes de management de la sécurité des systèmes d'information instituées par la suite ISO/IEC 2700x

- **Transfert de compétence**

  Assurer le transfert de compétence à un groupe de 15 personnes sur une durée de 5 jours sur le management de la sécurité et l'audit de la sécurité technique (normes : ISO/IEC 27002 et ISO 27001)

- **Identification de l'existant**

  Organiser des entretiens avec les parties prenantes pour identifier les lacunes et les bonnes pratiques déjà en place et d'en sortir la cartographie des données, des informations et des ressources.

- **Test des systèmes informatiques**

  Réaliser différents tests sur les systèmes du Trésor public en donnant des références par rapport aux normes et aux bonnes pratiques internationales, notamment :

  - Effectuer des tests de sécurité conformément au guide de test de sécurité Web OWASP (https://owasp.org/www-project-web-security-testing-guide/v42/)

- Réaliser des tests de piratage social/phising, présenter les résultats et les solutions proposées ;
- Tester pour s'assurer que le service conserve une disponibilité de 99,95 % et des temps de réponse inférieurs à 100 millisecondes pendant la haute saison, sans relâche excessive pendant les périodes normales, et/ou motiver explicitement tout écart proposé par rapport à cette norme ;
- Proposer une architecture et des processus spécifiques pour la surveillance et la détection des intrusions.

- **Rapport**

Rédiger les rapports des entretiens et des tests. Préconisations et propositions de solutions.

4. Résultats attendus et livrables de la mission

Indépendamment des différents documents intermédiaires qui doivent être produits, tels que les comptes rendus des réunions, les supports de présentation et de communication, les questionnaires…, le prestataire doit produire à la fin de chaque phase les livrables correspondants en format papier de 02 exemplaires et en format numérique standard (Word, PDF). Tous les livrables seront rédigés en langue française.

Au terme de la prestation, il est attendu du consultant les livrables suivants :

Phase	Durée	Livrables	Critères de vérification
Phase 1	125 jours après le commencement de la prestation	**L01** : Plan d'organisation et de réalisation de la mission, notamment : – Le plan d'assurance qualité ; – Le plan management de projet ; – Le planning détaillé du déroulement de la mission ; – Le support de formation ISO/IEC 27002 et ISO 27001	Pertinence – Exactitude – Priorité
		L02 : Rapport de l'étude de l'existant	Exactitude – Exhaustivité – Pertinence COBIT – ITIL – ISO/IEC 2700x
		L03 : Documents contenant : – Le guide des tests de sécurité (préalablement au développement, pendant la conception, pendant le développement, pendant le déploiement, maintenance et opération), – La planification, la découverte et l'exploitation ; – Le rapport des tests de sécurité (rapport d'audit organisationnel, rapport d'audit technique de la sécurité) et recommandations générales	Exactitude – Exhaustivité – Pertinence OWASP

		L04 : Document contenant : - Le plan de formation et les scenarios des tests de piratage social/ phishing; - Le guide des tests de simulation de piratage social/ phishing; - Le rapport des tests de simulation contenant minimalement une description détaillée de chacun de test effectué et des recommandations générales.	Pertinence – Exactitude – Priorité
		L05 : Document contenant : - La liste des fonctionnalités, des entrées utilisateurs, des types d'utilisateurs, le tout associé à des scénarios des charges avec le volume que l'on souhaite contrôler (Connexion, transaction, requêtes etc.) ; - Le processus des tests de performance et de la haute disponibilité, le cadrage et l'étude des entrants, le scripting, la modélisation et monitoring et la réalisation des tirs et analyse ; - Le rapport des tests de performance et de la haute disponibilité et des recommandations générales.	Pertinence – Exactitude – Priorité
		L06 : Document d'architecture IDS contenant minimalement : - Le fonctionnement de détection d'attaque (monitoring, analyse et transmission des résultats); - Le diagramme d'IDS - Les avantages et les limites ; - Le système de prévention d'intrusion (IPS) et son fonctionnement ; - La description de processus spécifique de l'IDS et de l'IPS avec les résultats de simulation	Pertinence – Exactitude – Priorité

Phase 2	40 jours après la validation des rapports relatifs à la Phase 1	**L07 :** Document contenant : - La synthèse des recommandations - Le plan d'actions détaillé proposant pour chaque vulnérabilité identifiée, les mesures correctives et préventives adéquates.	Pertinence – Exactitude – Priorité
Phase 3	100 jours après la validation des rapports relatifs à la Phase 2	**L08 :** Documents: - La politique sécurité des systèmes d'information ; - Le guide de sécurité des systèmes d'informations ; - Le manuel des procédures des systèmes d'informations ; - Charte d'utilisation des ressources informatiques ; - Support de sensibilisation ;	Pertinence – Exactitude – Priorité
		L09 : Rapport définitif de la mission	Pertinence – Exactitude – Priorité

Tous les documents et rapports produits par le titulaire dans le cadre de la présente mission sont la propriété exclusive du Trésor public.

5. Attendus de la réponse

a. Description de la démarche

Le cabinet devra décrire dans sa réponse la démarche proposée et la synthétiser dans la grille en annexe en décrivant :

- Les phases et les étapes associées
- Pour chaque étape, les activités et les livrables associés, ainsi que le délai

b. Description et profils du consultant

Le cabinet devra décrire dans la grille en annexe les différents critères concernant son profil

6. Profil du cabinet

Description du poste

L'auditeur de sécurité Informatique et Système d'Information a pour mission d'analyser et de diagnostiquer les systèmes d'information afin de les optimiser et de les rendre plus efficaces.

Missions :

- Assurer le transfert de compétence à un groupe de 15 personnes sur une durée de 5 jours sur le management de la sécurité et l'audit de la sécurité technique (normes : ISO/IEC 27002 et ISO 27001)
- Analyser / faire un état des lieux du système d'information, évaluer le matériel informatique et l'utilisation de l'informatique ;

- Établir un diagnostic sur le système d'information (technique, organisationnel, économique et humain)
- Analyser les différentes procédures (accès, sécurité, sauvegarde, récupération,…) et leur utilisation
- Identifier les améliorations à apporter, les nouvelles applications à concevoir et les points de sécurité informatique.
- Conseiller / recommander et accompagner dans la mise en place ou l'évolution des plateformes d'évaluations logicielles aussi bien les aspects méthodologiques que techniques et opérationnels ;
- Etudier et élaborer un plan d'actions dans l'évolutions et d'amélioration de ces plateformes ;
- Participer à la définition et à la mise en œuvre d'un dispositif permettant d'évaluer la qualité du test et du produit.
- Elaborer les procédures de sécurité des systèmes d'information

Compétences requises

Le personnel clé du cabinet devrait avoir les compétences suivantes :

- ISO/IEC 27002 et ISO 27001
- Architecture des systèmes d'information
- Flux d'information dans l'entreprise
- Différents systèmes informatiques
- Principaux modes de communications
- Principaux logiciels des systèmes d'information
- Sécurités SI
- Outils de gestion des exigences, de définition et de gestion de test;
- Cycle de vie d'un SI et de son processus de fabrication;
- Gestion et analyse des risques;
- Modèles d'évaluation et d'évolution des processus;
- Connaissance d'un ou plusieurs domaines fonctionnels;
- Méthodes de génération automatique de tests;
- Langue française (langue de rédaction du rapport)

Activités

- Bâtir une grille d'évaluation et apprécier les résultats obtenus
- Argumenter les décisions prises au regard des résultats et les défendre
- Contrôler les flux d'information dans l'établissement
- Reconnaître les points faibles d'un système d'information
- Concevoir des tests de sécurités
- Elaborer les procédures de sécurité des systèmes d'information

La présente prestation sera assurée par un consortium :

Le prestataire doit être un consortium composé au moins d'une firme internationale et d'une firme locale

Le consortium souhaitant soumissionner est tenu de justifier sa capacité technique à exécuter les travaux qui lui seront attribués, à travers ses expériences dans les 15 dernières années, notamment :

- 10 années d'expériences en Audit organisationnel de systèmes d'information ;
- 10 années d'expériences en Audit d'architecture informatique et de sécurité informatique;
- Avoir réalisé au moins un projet SI dans le domaine de la gestion des finances publiques ;

La firme locale en activité doit avoir :

- Une constitution légale dans le territoire national durant les CINQ dernières années au moins ;
- Avoir réalisé un Chiffre d'Affaires supérieur ou égal à 700 milles euros, durant la dernière année d'exercice (2021) ;

Le cabinet sera composé de :

- D'un chef de mission
- D'un auditeur en sécurité du système d'information
- D'un consultant en tests de performance

Critères de sélection :

Chef de mission

- Niveau de Formation :Avoir un niveau BAC + 5 en sciences et techniques de l'information, en informatique, ou dans un domaine similaire ;
- Avoir 10 ans d'expériences au moins et deux (02) expériences confirmées en matière d'audit de systèmes d'information et audit de sécurité de systèmes d'information ;
- Expériences spécifiques dans le domaine de l'audit des systèmes informatiques, sécurité et réseaux informatiques. Solides connaissances des outils d'évaluation de gouvernance informatique (COBIT 5, ITIL)
- Avoir une bonne connaissance de la norme ISO 2700x
- Ayant réalisé au moins une prestation portant sur la rédaction de cahier de charges / réalisation de schéma directeur informatique / élaboration de politique de sécurité / définition de procédures informatiques ;
- Avoir une bonne connaissance des maîtrises d'ouvrage en informatique et Gestion de projet ;
- Expériences dans le domaine d'analyse de risque et d'opportunités et de choix stratégiques ;
- Qualité d'analyse et de rédaction avec une réelle expertise technique ;
- Avoir la capacité prouvée d'assurer le transfert des compétences.

Consultant auditeur en sécurité du système d'information

- Niveau de formation : Diplôme d'ingénieur, avec une spécialisation en Sécurité des Systèmes d'Information et informatiques, en réseaux et télécommunication ou en Cryptologie.
- Expériences générales : Forte connaissance en management de la sécurité et le rôle de l'audit interne dans celui-ci et maîtrisez des normes ISO 45001 et ISO 19011
- Maîtrise des normes et des procédures de sécurité, des outils et des technologies relatifs à la sécurité informatique (ISO/IEC 2700x, COBIT 5, PCI-DSS etc.)
- Solides connaissances des outils d'évaluation et d'analyse de risques (systèmes et réseaux) et des méthodologies (OWASP, EBIOS).

- Qualité d'analyse et de rédaction avec une réelle expertise technique

Deux (02) Consultants expert en tests de performance et de robustesse

- Niveau de formation : Avoir un niveau BAC +5 en informatique ou expérience équivalente ;
- Avoir une expérience d'environ 5 ans en ingénieriede tests de performance et robustesse;
- Avoir un profil de développeur / génie, en systèmes et réseaux, cloud et big data ;
- Maîtriser les technologies et langages suivants :
    - JAVA, PYTHON, PHP
    - SGBD : Oracle, MySQL, PostGreSQL
    - OS : Windows Server et Linux (Ubuntu, Oracle Linux, …)
    - Réseaux : WAN, LAN, VLAN ainsi que des services TCP/IP (DNS, Firewall, Email, FTP, Annuaire, VPN, etc…)
- Ayant été formé en cybersécurité, technique de piratage (hacking) serait un atout
- Ayant obtenu une certification de niveau international (OSCP, CISSP, CISM, …) serait un atout
- Ayant réalisé les chantiers et les projets de tests de performance
- Ayant rédigé des plans de tests
- Ayant défini des modèles de charge
- Ayant développé des scripts, notamment des scripts à forte complexité
- Ayant exécuter des campagnes de tirs
- Ayant mis en place du monitoring et analyse des résultats
- Ayant produit des reportings des campagnes de test
- Ayant réalisé des dossiers de capitalisation et d'historisation

7. Durée de la prestation

La prestation durera 8 mois.

Annexes

A. Grille de description de la démarche

N°	*Intitulé de la phase*	*Description de la phase*	*Description des étapes*	*Livrables*	*Délai*
1	*Nom de la phase*	*Etapes à réaliser*	*Activités à réaliser*	*L01...*	*S0 +1*

B. Grille de description du parcours du cabinet

Domaines	**Description avec expériences selon le domaine**	**Pondération si applicable**
Les références professionnelles	En rapport avec des missions d'audit organisationnel, technique et sécurité du système d'information d'une entreprise ou d'une organisation de même nature	
La qualité du prestataire	CV de l'équipe qui va intervenir pour la mission, avec leur expérience dans des missions d'audit organisationnel, technique et sécurité d'une entreprise ou domaine de même nature ;	
La méthodologie proposée	Modalités, description des outils et méthodes utilisés pour assurer la prestation (déroulement des entretiens...);	
Le calendrier de travail	Calendrier proposé avec le nombre de journées de travail pour réaliser la prestation sur la période définie ;	